UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/573,684	01/04/2007	Yuichi Futa	2006_0401A	3546

52349 7590 03/30/2009

WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
03/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/573,684	FUTA ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 March 2009*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,5 and 10-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,5,10-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/18/09 has been entered.

Claims 1, 2, 4, 5 and 10-12 are pending. Claims 1, 2, 11, and 12 have been amended.

Response to Arguments

Applicant's arguments with respect to claims 1, 2, 11, and 12 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

Claims 1, 2, 11, and 12 are objected to because of the following informalities: the steps of the claims reuse the same labels. In other words, (i), (ii), and (iii) are all used to define two steps. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The term "the communication device" is undefined. It lacks antecedent basis and does not correctly refer to any previously defined entities.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 2, 5, 10, 11, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP 5,371,794 to Diffie et al., hereinafter Diffie in view of "Keying Hash Functions for Message Authentication", 1996 publication by Bellare et al., hereinafter Bellare.

As per claims 1, 2, 11, and 12, Diffie teaches a communication system, device, and method between a first device and a second device, wherein the first device [base]

(i) encrypts a 1st key [RN1] using a public key of the second device [mobile] to generate 1st encrypted data, and transmits the 1st encrypted data to the second device (col. 7, lines 50-65)),

(ii) receives 2nd encrypted data from the second device, and decrypts the 2nd encrypted data using a secret key of the first device to obtain a 2nd key [RN2], and (col. 8, lines col. 49-53))

(iii) generates, based on the 1st and 2nd keys, a 1st encryption key [session key] for use in communication with the second device, the second device (col. 8, lines 65-67)

(i) encrypts a 3rd key [RN2] using a public key of the first device to generate the 2nd encrypted data, and transmits the 2nd encrypted data to the first device (col. 8, lines 49-57)),

(ii) receives the 1st encrypted data from the first device, and decrypts the 1st encrypted data using a secret key of the second device to obtain a 4th key [RN1] (Fig. 5a and col. 8, lines 44-45), and

(iii) generates, based on the 3rd and 4th keys, a 2nd encryption key [session key] for use in communication with the first device (col. 8, line 47-49), and the first and second devices perform encrypted communication using the 1st and 2nd encryption keys (col. 8, lines 47-49),

wherein the first device generates the first encryption key based on the first and second keys (col. 8, lines 65-67).

Diffie teaches the first device encrypts the first transmission data using the first encryption key to generate encrypted first transmission data, and transmits the

encrypted first transmission data to the second device (col. 9, lines 15; session key is obtained, inherently used to encrypt data). Diffie teaches the second device generates the second encryption key based on the third and fourth keys (col. 8 ,lines 47-49), receives from the communication device the encrypted first transmission data, decrypts the encrypted first transmission data using the second encryption key (col. 9, lines 15; session key is obtained, inherently used to decrypt data). Again Diffie's invention is directed to two parties obtaining a session key whereby data may be encrypted and decrypted. Diffie teaches the use of a encrypted check sum field but is silent in teaching creating a first/second hash key (same key) and using the hash key to hash the data to created a hash value, sending this hash value to the second device so that it may verify that the data has not been tampered with. The use of MAC and their corresponding keys is well known in the art. In order for MAC to work both sides need to know the key being used. Diffie teaches the first and second keys RN1 and RN2 are known to each side of the communication. In fact they jointly arrive at these keys. While the claims label the second device's keys as the third and fourth keys, they are in fact the same as the first and second keys. Bellare teaches the NMAC algorithm in section 4 starting on page 10. This NMAC algorithm uses two keys in the generation of the MAC [first hash value]. MACs again are known in the art to provide tampering evidence. Because the NMAC uses two keys, this algorithm would suit Diffie's system well. Diffie generates two keys known to both sides of the communication (RN1 and RN2). It is within the capabilities of one of ordinary skills in the art to substitute known methods for known purposes which result in predictable results. One of ordinary skill in

the art could have substituted the NMAC algorithm for the check sum to increase the security of the system. The use of MAC is more secure than simple check sums. Substituting this teaching into Diffie would render the claims obvious. It is obvious that the NMAC algorithm would use RN1 and RN2 (or with padding to achieve the desired bit length) to hash the data. The second device would then receive the resulting hash value [first hash value] and compare that value to its own hash value [second hash value] which is calculates by hashing the received data with its copy of RN1 and RN2. Furthermore the session key of Diffie [first/second encryption key] is distinct from the hash key. The hash key would be equal to RN1 and RN2. The encryption key is equal to RN1 XOR RN2.

As per claim 5, the combined system of Diffie and Bellare teaches the key generation unit performs an exclusive OR operation using the 1st and 2nd keys (Diffie, col. 8, lines 47), and generates the encryption key and the hash key based on a result of the operation. Diffie XOR's the key parts to create the session key. Examiner relies on the rationale to combine Diffie and Bellare as disclosed above for using a hash key.

As per claim 10, Diffie teaches the data generation [packet] unit encrypts the 1st key [RN1] based on a key encapsulation mechanism to generate the 1st encrypted key data, and the decryption unit decrypts the 2nd encrypted key data based on a key decryption mechanism to obtain the 2nd key [RN2] (col. 9, lines 57-63).

Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over Diffie and Bellare as applied to claim 2 above, and further in view of USP Application Publication 2003/0093669 to Morais et al., hereinafter Morais.

As per claim 4, Diffie and Bellare do not explicitly teach the key generation unit concatenates the 1st and 2nd keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the encryption key and the hash key based on the hash value. Morais teaches the key generation unit concatenates the 1st and 2nd keys to generate concatenated data, calculates a hash value for the concatenated data, and generates the encryption key and the hash key based on the hash value [0052]. Diffie and Bellare teach using XOR to combine the key parts. Concatenation as taught by Morais of key parts is yet another way to logically combine keys to arrive at another key. This is just a simple substitution of a known function and as such it would have been obvious to one of ordinary skill at the time the invention to substitute another known logical way of combining keys. The combining rationale of Diffie and Bellare is again relied upon to use the newly formed encryption and hash key to generate hash values (MAC).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2431